| **Department of Economic Security**<br>Information Technology Standards | Title: 1-38-0029 Information Technology (IT) and Office Equipment and Resources Acceptable Use Policy | |
|---|---|---|
| *Subject*: This policy defines acceptable use of Information Technology (IT) and office equipment and resources by DES employees. | ***Effective Date:***<br>09/05/01 | ***Revision:***<br>1.5 |

1. **Summary of Policy Changes**
   1.1. 08/14/02 – Text forbidding chain letters and "spam" was added as 6.3.8 and 6.3.9, at the Office of Data Security's suggestion.
   1.2. 05/02/03 – Addition of a Reference to A.R.S. §, 38-448 State employees; access to internet pornography prohibited; cause for dismissal; definitions.
   1.3. 05/11/04 – Added text about telephone usage monitoring rules in 6.4., and downloading or installing software in 6.3.10, 6.3.11, and 6.3.12.
   1.4. 04/27/05 – Added text prohibiting political messages.
   1.5. 02/21/06 – Added text prohibiting use or visiting of gambling websites using DES equipment.

2. **Purpose**
   This policy defines acceptable use of Information Technology (IT) and office equipment and resources by DES employees and all others with access to DES facilities, equipment and/or systems.

3. **Scope**
   This policy applies to all DES administrative entities, councils, divisions, administrations, and programs.

4. **Responsibilities**
   4.1. The DES Director, Deputy Directors, Associate Director, and Assistant Directors are responsible for implementing and enforcing this policy.
   4.2. The DES CIO is responsible for implementing this policy, as regards IT equipment.
   4.3. The DES Division of Technology Services is responsible for implementing this policy and monitoring DES compliance, as regards IT equipment.
   4.4. The DES Managers and Supervisors are responsible for monitoring compliance and acceptable use.

5. **Definitions and Abbreviations**
   5.1. **Definitions**
      5.1.1. IT Equipment includes, but is not limited to:
         5.1.1.1. Personal Computers (PC), including desktops, laptops, and PDAs.
         5.1.1.2. Network Computers (NC).
         5.1.1.3. IT Peripherals, including scanners, printers, and faxes.
         5.1.1.4. Telephony equipment, including telephones, wireless (cell) phones, and pagers.
      5.1.2. IT Resources includes, but is not limited to:
         5.1.2.1. Internet, access to the World Wide Web (WWW).
         5.1.2.2. Intranet, access to an internal Internet system.

5.1.2.3. Extranet, access to an internal system by designated participants, such as providers, vendors, and external customers.

5.1.2.4. Electronic Mail.

5.1.3. Office Equipment includes, but is not limited to:

5.1.3.1. Fax machines, copiers, and telephones.

5.2. **Abbreviations**

5.2.1. **CIO** – **C**hief **I**nformation **O**fficer

5.2.2. **DTS** – **D**ivision of **T**echnology **S**ervices

5.2.3. **DES** – **D**epartment of **E**conomic **S**ecurity

5.2.4. **GITA** – **G**overnment **I**nformation **T**echnology **A**gency

5.2.5. **IT** – **I**nformation **T**echnology

5.2.6. **PDA** – Personal Digital Assistant

5.2.7. **NC** – Network Computer

5.2.8. **PC** – Personal Computer

## 6. POLICY

DES policy for the acceptable use of DES IT and office equipment and resources is:

6.1. IT and office equipment and resources are provided to assist employees in accomplishing their work. Use of these resources imposes responsibilities and obligations on employees and is subject to State and Department policies and local, state and federal laws.

6.2. **Acceptable use** of IT and office equipment and resources is limited to:

6.2.1 Work related activities as defined by DES management.

6.2.2. Department training activities that are considered "career enhancing" or are directly work related.

6.2.3. Any personal use that does not:

6.2.3.1.Consume more than an insignificant amount of time or resources,

6.2.3.2.Fall outside of reasonable duration and frequency,

6.2.3.3.Interfere with staff productivity,

6.2.3.4.Adversely affect the performance of official duties by the employee,

6.2.3.5.Preempt any business activity.

6.3.**Unacceptable use** of IT and office equipment and resources includes:

6.3.1 Private business activities,

6.3.2 Solicitation for personal profit or gain,

6.3.3 Viewing or downloading of obscene (explicit sexual) materials, (See 9. References)

6.3.4 Copyright infringement,

6.3.5 Sexual harassment,

6.3.6 Discriminatory and defamatory activities,

6.3.7 Any deceptive, fraudulent, malicious or illegal activity.

6.3.8 Perpetuate chain e-mail letters or their equivalents. This includes letters that require the recipient to forward an e-mail to a specified number of addresses in order to achieve some monetary, philosophical, political, superstitious, or other goal. E-mails that are part of a multilevel marketing or pyramid-selling scheme, sometimes

known as "Ponzi schemes," are illegal in many places and are specifically forbidden under this policy.

6.3.9 Create and/or send "spam". Spam is defined as any unsolicited electronic communication that is sent to any number of recipients who did not specifically request or express an interest in the material advertised in the communication.

6.3.10 Downloading, installing, and/or using any software or program not specifically authorized by your (local) IT management.

6.3.11 Downloading, installing, and/or using any image or other file not specifically related to your job duties or authorized by your management.

6.3.12 Bringing discredit on the State in your operation and use of information technology and office equipment and resources.

6.3.13 Creating or distributing messages that promote or support political parties, positions, or activities.

6.3.14 Use or visiting of gambling websites.

6.4 **Use of Internet, Intranet, Extranet and E-mail** services and resources provided by the Department will be subject to monitoring for compliance, security, and/or network management.

Internet and E-mail Monitoring may include:

6.4.1. The logging of which users access which Internet resources and web sites.

6.4.2. Reviewing E-mail content.

Managers can monitor the ***usage*****, i.e. amount of time spent on the phone, long distance calls, inappropriate calls**, etc., but no authority is granted in this policy to record the ***content*** of calls made while on the States' time. Should managers have a concern as to the content of phone messages, they should contact the personnel office for further guidance.

The DSA, OSI, DES Attorney Generals' Office, and the personnel office have a unanimous consensus on this clarification of the monitoring policy.

## 7. Implications

7.1. This policy replaces all previous DES policy on the topics of the use of IT and office equipment and resources.

## 8. Implementation Strategy

8.1. When this policy is adopted, all related data security and personnel forms and policies must be revised to comply with this new policy.

## 9. References

| | |
|---|---|
| 9.1. A.R.S. §, 38-448 | State employees; access to internet pornography prohibited; cause for dismissal; definitions |
| 9.2. A.R.S §, 41-772 | Prohibitions; violation; classification; civil penalty; protection of civil or political liberties |
| 9.3.A.R.S. §, 13-3301(7) | Social gambling means gambling that is not conducted as a business and that involves players who compete on equal terms with each other in a gamble if…. (See 5.1.4 Social Gambling definition) |
| 9.4 A.R.S. §, 13-3302(A) | In a lottery or football pool where all the players are over 21 and where all the players would receive is their share of the winnings |

with no extra “cut” or portion of winnings for the organizer, the activity is social gambling, and it is not a crime.

**10. Attachments**

10.1 None

**11. Associated GITA IT Standards or Policies**

11.1 P501 Rev 1.0 Internet Use

11.2 P401 Rev 1.0 Email Use

**12. Review Date**

12.1 This document will be reviewed twelve (12) months from the original adoption date and every twelve months thereafter.